201410243

Smartphone Smart Card

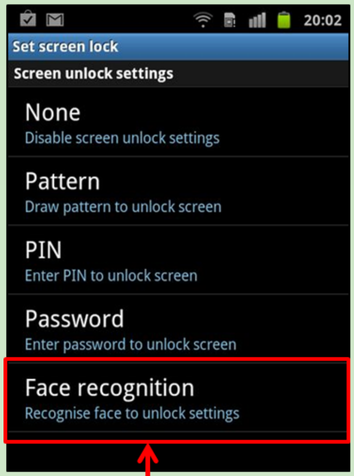
Do's and Don'ts

- Smartphones are not impenetrable. Secure your smartphone with a password, and utilize apps such as *Find My iPhone* and *AndroidLost* to locate lost or stolen devices.
- All smartphones have cameras and microphones that can be remotely activated. Caution should be used when smartphone is near sensitive information.
- Bluetooth and wireless capable smartphones are convenient but easily exploitable by hackers. Use a VPN if possible and avoid public wireless networks, especially when accessing sensitive information.
- Prior to downloading apps on your smartphone, read the developers permissions. Many apps now require permission to access your camera, microphone, text messages, and phone contacts.
- Keep your locations services turned off until they are actually needed. Otherwise, your daily movements are likely being tracked.
- If you have a google account, you can use your google credentials to login at maps.google.com/locationhistory to see your phones location history for the last year or more.

Physical Exploitation

The first line of defense in preventing unauthorized access to your data is to protect your smartphone with a passcode. Each operating system has different methods of security, both achieving the same goal. Always set your smartphone to require a passcode immediately and use an alpha-numeric passcode.

Android 4.4.4



20:02

Set screen lock

Screen unlock settings

None
Disable screen unlock settings

Pattern
Draw pattern to unlock screen

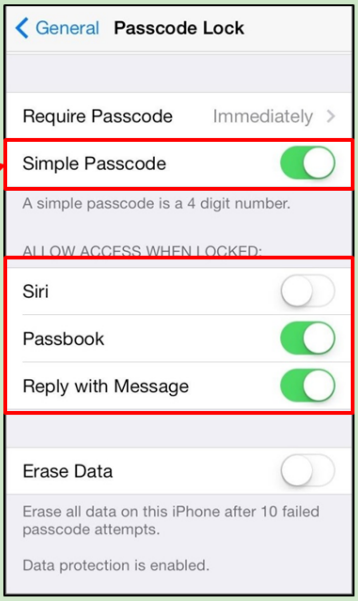
PIN
Enter PIN to unlock screen

Password
Enter password to unlock screen

Face recognition
Recognise face to unlock settings

Face Unlock is not secure; a picture of you will allow access to your phone.

iPhone 8.0.2



General Passcode Lock

Require Passcode Immediately

Simple Passcode

A simple passcode is a 4 digit number.

ALLOW ACCESS WHEN LOCKED:

Siri

Passbook

Reply with Message

Erase Data

Erase all data on this iPhone after 10 failed passcode attempts.

Data protection is enabled.

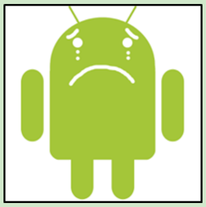
DISABLE Simple Passcode and secure device with a longer alpha-numeric passcode.

Turn these settings OFF; they allow anyone to access areas of your phone without a passcode.

Lost/Stolen Phone

In the U.S., it has been reported that over 100 cell phones are stolen or lost every minute. This fact alone proves it is necessary to keep your device secure and locked with a passcode. There are apps available for both Android and iPhone platforms that allow the user to manage their smartphones remotely in the event their phone is stolen or lost.

Android 4.4.4



Androidlost

- Wipe phone
- Lock phone
- Erase SD Card
- Locate by GPS or Network
- Email when SIM is charged
- Take picture
- Record sound from microphone
- Google.com/device

iPhone 8.0.2

Find My iPhone

- Wipe phone
- Lock phone
- Activate alarm
- Activate camera
- Locate by GPS or Network
- Backup data through iCloud

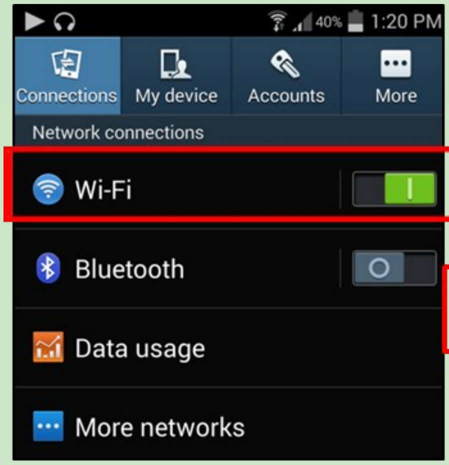
Smartphone Smart Card

201410243

Wireless Networks

If possible, public Wi-Fi networks should be avoided due to the risk of interception by third parties. If public networks must be used, avoid logging into accounts that require passwords, as log-in credentials are easily exploited by hackers. Always use a VPN client to encrypt on-line transactions.

Android 4.4.4



40% 1:20 PM

Connections | My device | Accounts | More

Network connections

Wi-Fi ON

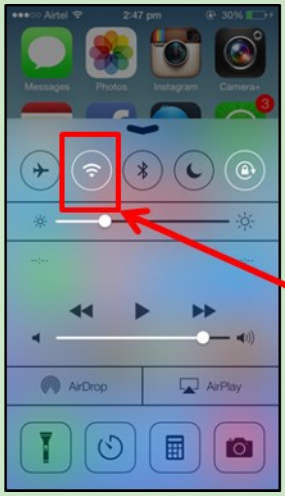
Bluetooth OFF

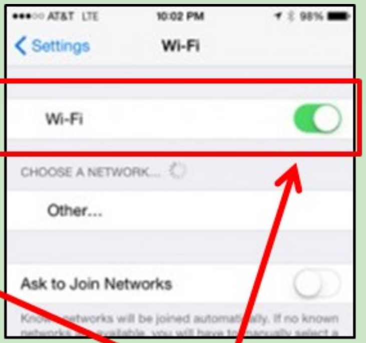
Data usage

More networks

DISABLE Wi-Fi when not in use.

iPhone 8.0.2





AT&T LTE 10:02 PM 98%

Settings Wi-Fi

Wi-Fi ON

CHOOSE A NETWORK...

Other...

Ask to Join Networks OFF

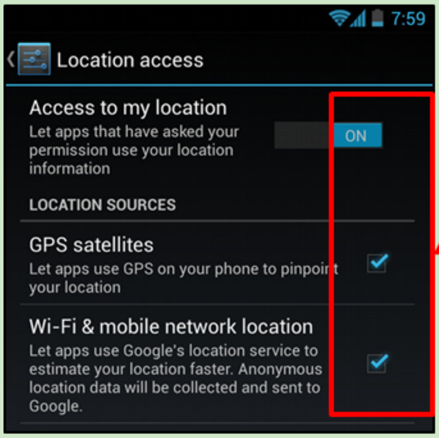
Known networks will be joined automatically. If no known networks are available, you will have to manually select a

From the Control Center or under Settings, DISABLE Wi-Fi when not in use.

Location Tracking

Many applications will ask permission to use your current location. Users should avoid granting access when possible. Turn off all location services when they are not in use.

Android 4.4.4



7:59

Location access

Access to my location ON
Let apps that have asked your permission use your location information

LOCATION SOURCES

GPS satellites ☑
Let apps use GPS on your phone to pinpoint your location

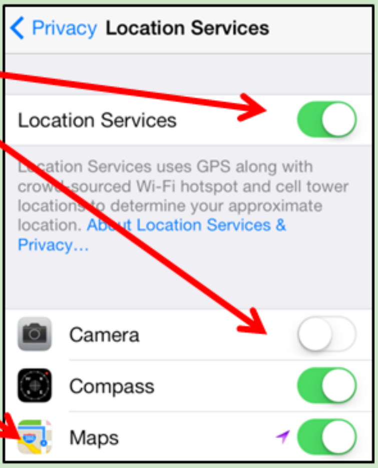
Wi-Fi & mobile network location ☑
Let apps use Google's location service to estimate your location faster. Anonymous location data will be collected and sent to Google.

DISABLE location services when not in use.

iPhone 8.0.2

DISABLE location services when not in use, including Camera tools which geotag photos and store this information within EXIF data.

Only grant access to apps that require a location to function.



Privacy Location Services

Location Services ON

Location Services uses GPS along with crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location. About Location Services & Privacy...

Camera OFF

Compass ON

Maps ON

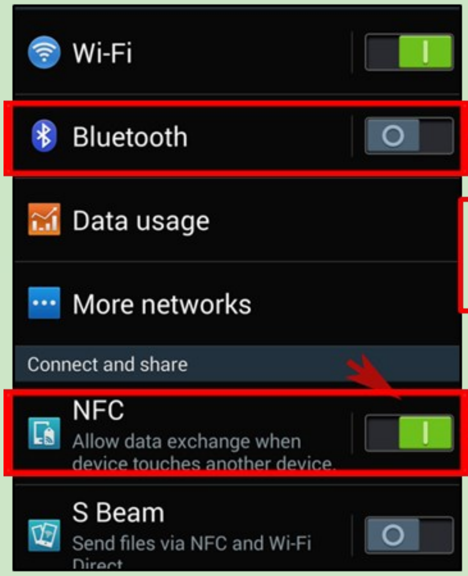
Smartphone Smart Card

201410243

Bluetooth

Bluetooth is a wireless technology standard for exchanging data over short distances from fixed and mobile devices. When Bluetooth is enabled on your smartphone, hackers could gain entry to your device and obtain contacts, messages, calendars, photos, and notes without you even knowing.

Android 4.4.4



Wi-Fi I

Bluetooth O

Data usage

More networks

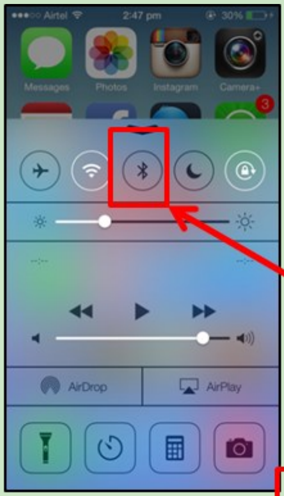
Connect and share

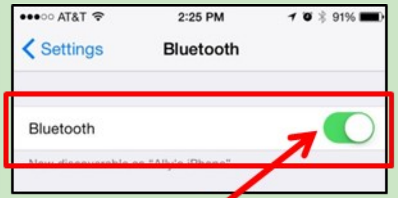
NFC
Allow data exchange when device touches another device I

S Beam
Send files via NFC and Wi-Fi Direct O

DISABLE Bluetooth and NFC Sharing when not in use.

iPhone 8.0.2





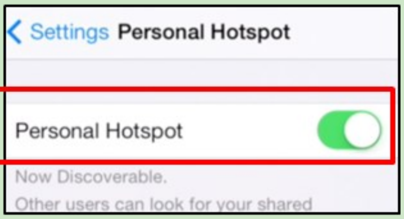
●●●○○ AT&T 2:25 PM 91%

Settings Bluetooth

Bluetooth

Now discoverable as "Ally's iPhone"

From the Control Center or under Settings, DISABLE Bluetooth when not in use.



Settings Personal Hotspot

Personal Hotspot

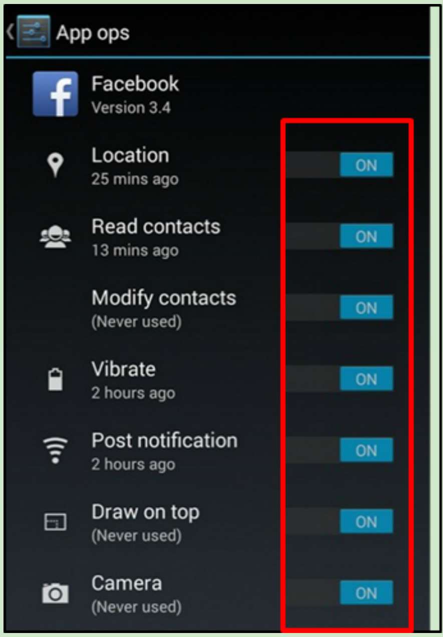
Now Discoverable.
Other users can look for your shared

Never share your internet connection.

Data Retaining Applications

Downloaded applications often collect users' personal information (e.g. name, email addresses, contacts lists, credit card numbers, device information, etc.) and allow third parties to access this private and sensitive data. Even personal assistant applications, like Siri and Google Now, collect and retain user data. Siri voice clips are transferred to Apple's data farm and kept for up to two years. Google Now collects data from web searches, calendar appointments, photos, contacts, text messages, shopping habits, and book/movie/music choices. Review and manage applications to see what information is being collected and what permissions you have allowed.

Android 4.4.4



App ops

Facebook
Version 3.4

Location
25 mins ago ON

Read contacts
13 mins ago ON

Modify contacts
(Never used) ON

Vibrate
2 hours ago ON

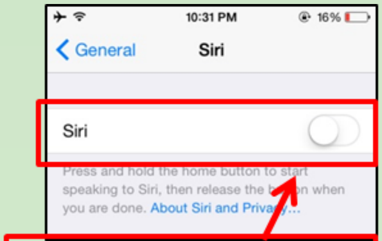
Post notification
2 hours ago ON

Draw on top
(Never used) ON

Camera
(Never used) ON

Permissions management, through Apps Ops or third-party tools, are possible with Android 4.4.2 and up only with root access to the device.

iPhone 8.0.2



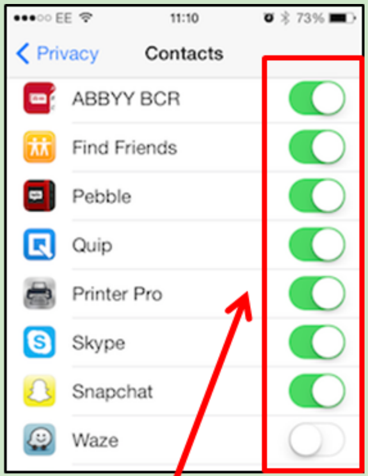
10:31 PM 16%

General Siri

Siri

Press and hold the home button to start speaking to Siri, then release the button when you are done. About Siri and Privacy...

Once Siri is DISABLED, all identifiers and associated data are deleted immediately.



●●●○○ EE 11:10 73%

Privacy Contacts

ABBYY BCR

Find Friends

Pebble

Quip

Printer Pro

Skype

Snapchat

Waze

Turn OFF access for apps that you do NOT want using your information.